CLAIMS

1. A method comprising:

collecting entropy data;

storing the entropy data in a nonvolatile memory;

updating the entropy data stored in the nonvolatile memory with newly collected entropy data; and

generating a string of random bits from the entropy data stored in the nonvolatile memory.

2. A method as recited in claim 1 wherein the entropy data is collected from multiple sources.

3. A method as recited in claim 1 wherein the entropy data is collected from multiple sources within a computer system.

4. A method as recited in claim 1 wherein the entropy data includes data related to a processor in a computer system.

5. A method as recited in claim 1 wherein the entropy data includes data related to an operating system executing on a computer system.

6. A method as recited in claim 1 wherein the entropy data is maintained in a protected portion of an operating system kernel.

7. A method as recited in claim 1 wherein the method is executing on a system and the entropy data is inaccessible by an application program executing on the system.

8. A method as recited in claim 1 wherein generating a string of random bits includes hashing the entropy data to generate random seed data.

9. A method as recited in claim 1 wherein updating the entropy data stored in the nonvolatile memory includes collecting new entropy data at periodic intervals.

10. A method as recited in claim 1 further including communicating the string of random bits to an application program requesting a random number.

11. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 1.

12. A method comprising:

receiving a request for a random number;

retrieving entropy data from a nonvolatile memory device, wherein the entropy data is regularly updated with newly collected entropy data;

hashing the entropy data to create random seed data;

generating a string of random bits from the random seed data; and

12) cw/o

communicating the string of random bits to the requester of the random number.

13. A method as recited in claim 12 wherein the entropy data is collected from multiple sources within a computer system.

14. A method as recited in claim 12 wherein the entropy data includes data related to a state of a processor in a computer system and data related to a state of an operating system executing on the computer system.

15. A method as recited in claim 12 wherein the entropy data is maintained in a protected portion of an operating system kernel.

16. A method as recited in claim 12 wherein the random seed data is maintained in a protected portion of an operating system kernel.

17. A method as recited in claim 12 wherein the entropy data is inaccessible by the requester of the random number.

18. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 12.

19. A method comprising:

collecting entropy data;

storing the entropy data in a protected portion of an operating system kernel; and

generating a string of random bits based on the entropy data.

20. A method as recited in claim 19 wherein the entropy data is collected from multiple sources.

21. A method as recited in claim 19 wherein the entropy data is inaccessible by an application program.

22. A method as recited in claim 19 further comprising updating the entropy data with newly collected entropy data.

23. A method as recited in claim 19 further comprising communicating the string of random bits to an application program requesting a random number.

24. One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 19.

25. An apparatus comprising:

a nonvolatile memory configured to store entropy data, wherein the entropy data stored in the nonvolatile memory is updated regularly; and

2/4/05

a random number generator coupled to the nonvolatile memory, wherein the random number generator utilizes the entropy data stored in the nonvolatile memory to generate strings of random bits.

26. An apparatus as recited in claim 25 wherein the entropy data is collected from multiple sources.

27. An apparatus as recited in claim 25 wherein the entropy data is updated at periodic intervals.

28. An apparatus as recited in claim 25 wherein the entropy data is maintained in a protected portion of an operating system kernel such that the entropy data is inaccessible by an application program.

29. An apparatus as recited in claim 25 wherein the entropy data includes data related to a processor in a computer system and an operating system executing on the computer system.

30. An apparatus as recited in claim 25 wherein the random number generator hashes the entropy data to generate random seed data.

31. An apparatus as recited in claim 25 further including a timer coupled to the random number generator, the timer indicating when to update the entropy data stored in the nonvolatile memory device.

32. One or more computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to:

collect entropy data from multiple sources;

store the collected entropy data in a nonvolatile memory;

update the entropy data stored in the nonvolatile memory with newly collected entropy data; and

produce a string of random bits from the entropy data stored in the nonvolatile memory.

33. One or more computer-readable media as recited in claim 32 wherein the entropy data includes data related to a state of one or more processors.

34. One or more computer-readable media as recited in claim 32 wherein the entropy data is maintained in a protected portion of an operating system kernel.

35. One or more computer-readable media as recited in claim 32 wherein the entropy data includes data related to a state of an operating system executing on a computer system.

~~**36.** One or more computer-readable media as recited in claim 32 wherein to produce a string of random bits from the entropy data, the one or more processors hash the entropy data to generate random seed data.~~

~~**37.** One or more computer-readable media as recited in claim 32 wherein the entropy data stored in the nonvolatile memory is updated with newly collected entropy data at periodic intervals.~~